UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/805,279	03/13/2001	Robert M. Barnhart	SAIC0039	1264

27510 7590 07/11/2006

KILPATRICK STOCKTON LLP
607 14TH STREET, N.W.
WASHINGTON, DC 20005

EXAMINER	
JARRETT, SCOTT L	

ART UNIT	PAPER NUMBER
3623	

DATE MAILED: 07/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/805,279	BARNHART, ROBERT M.	
	Examiner	Art Unit	
	Scott L. Jarrett	3623	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *29-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *29-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This **Final** Office Action is in response to Applicant's amendment filed June 2, 2006. Applicant's amendment amended claims 29-32. Currently Claims 29-33 are pending, Claims 1-28 being previously canceled.

Response to Amendment

2. The Objection to the Title in the previous Office Action is withdrawn in response to Applicant's amendment to the Title.

The 35 U.S.C. 112(2) rejection(s) of Claims 29, 20 and 33 are withdrawn.

Response to Arguments

3. Applicant's arguments filed June 2, 2006 have been fully considered but they are not persuasive. Specifically Applicant's argue, see remarks filed June 2, 2006:

- that the prior art of record, specifically Shrader et al., fails to teach or suggest each and every element of the claimed invention, specifically failing to teach or suggest:
  - an architecture requiring only two entities a voting entity and a server (Paragraph 1, Page 8);
  - associating the cast ballot and server's digital signature of the cast ballot with a vote serial number (Last Paragraph, Page 8);
  - forming a confirmation token comprising the server's digital signature of the cast ballot and the vote serial number (Paragraph 2, Page 9);

- making the confirmation token available to a user (Paragraph 3, Page 9);
- receiving a confirmation token made available to a user (Paragraph 4, Page 9);
- extracting the vote serial number and the server's digital signature from the received token (Last Paragraph, Page 9); and
- comparing the server's digital signature received, the server's digital signature using its private key and the server's digital signature using its public key (Paragraph 2, Page 10).

- that the prior art of record, specifically Cranor et al. in view of Shrader et al., fails to teach or suggest each and every element of the claimed invention, specifically failing to teach or suggest:

- forming a digital signature of the cast ballot using the private key of the voter (Paragraph 1, Page 11);
- forming a digital signature of the cast ballot using the private key of the server (i.e. different keys are used to form the two digital signatures; Paragraph 1, Page 11);
- associating the cast ballot, voter's digital signature of the cast ballot and server's digital signature of the cast ballot with a vote serial number (Paragraph 2, Page 11);
- a confirmation token comprising the voter's digital signature of the cast ballot, the server's digital signature of the cast ballot, the cast ballot,

the vote serial number and the digital signature of the above elements (aggregation, Last Paragraph, Page 11); and

- that the combination of Cranor et al. and Shrader et al. is an indication of improper hindsight (Paragraph 2, Page 12).

In response to Applicant's attempt to traverse the Official Noticed facts in the previous Office Action(s) (Paragraph 2, Page 6) is inadequate. Specifically Applicant's attempt at traversing the Official Notice findings as stated in the previous Office Action(s) (Remarks: Paragraph 2, Page 6) is inadequate wherein an adequate traversal is a two-step process. First, Applicant's must state their traversal on the record. Second and in accordance with 37 C.F.R. 1.111(b) which requires Applicant's to specifically point out the supposed errors in the Office Action, Applicant's must state why the Official Notice statement(s) are not to be considered common knowledge or well known in the art.

In this application, while Applicant's have clearly met step (1), Applicant's have failed step (2) since they have failed to argue why the Official Notice statement(s) are not to be considered common knowledge or well known in the art. Because Applicant's' traversal is inadequate, the Official Notice statement(s) are taken to be admitted as prior art. See MPEP 2144.03.

Specifically it has been established that it was old and well known in the art at the time of the invention:

- to represent a document as an image (e.g. graphical ballot);

- to use one-way hash functions for data integrity in conjunction with digital signature schemes;

- that cryptographic hash functions generate a hash-value which serves as a compact representative image (imprint, digital fingerprint, message digest) of an input string that can be used to uniquely identify the hashed message/string;

- that X.509 is a known digital certificate standard; and

- that signing a message provides a mechanism for determining the authenticity and integrity of a message.

Further it is noted that none of the Officially Noticed facts listed above are used in the current rejection of the pending claims.

In response to the Applicant's argument that the prior art of record fails to teach each and every element of the claimed invention the examiner respectfully disagrees.

As an initial matter it is noted that the invention, as claimed, merely recites the old and very well known process of sharing and validating any text, whether that text is a ballot, an image of the ballot, a message, a document, or the like, wherein the method/system enables any two "entities" to "share" information in a secure and verifiable manner, regardless of the intended use of the message (e.g. cast ballot). Thereby making the cast ballot, vote serial number and the like merely non-functional descriptive material, which is not materially, involved in the method steps (i.e. one could substitute any message/text in place of the cast ballot and/or vote serial number and the method steps would be unaltered). If the cast ballot and vote serial number were used

during the method steps, for example to ensure that a ballot is not cast twice as is taught by Shrader et al. (Paragraphs 0061-0063, Figures 7-8), then the data would cease to be non-functional descriptive material.

Specifically the well known process for securely sharing information between at least two entities, as evidenced by at least Shrader et al. (Paragraphs 0050-0053, 0058, 0060-0063; Figures 6-8), Cranor et al. (Paragraph 2, Page 5; "Tallier", Page 8; Last Paragraph, Page 10; Paragraph 1, Page 11; Figures 1-3); Challener et al., U.S. Patent No. 6,081793 (Columns 9-10; Figures 9A-9E; VoteHere.net "Digital Signature", Pages 17-18; Menezes et al., Handbook of Applied Cryptography, Pages 428-432), comprises:

- Sender
    - authoring/creating/generating a message/text;
    - digitally signing the message using the sender's private key
    - generating a "fingerprint" of the message using a hash (or other one-way) function;
    - encrypting the hash number/fingerprint using the sender's private key;
    - encrypting the message/text using the recipient's public key;
    - sending the encrypted message and digital signature;
- Recipient
    - receiving the encrypted message and digital signature;
    - extracting the encrypted message and digital signature;
    - verifying the message/signature;

- generate the message by decrypting the encrypted message using the recipients private key;
- generating a "fingerprint" of the received message by hashing the decrypted message;
- generating a "fingerprint" of the received message by decrypting the senders digital signature using the sender's public key (i.e. hash number); and
- comparing the two "fingerprints" to determine if they are equal and then determining that the message is verified if they are equal (i.e. was from the sender and was not tampered with during transit).

In response to Applicant's argument that the prior art of record fails (Shrader et al.) to teach of suggest an "architecture" requiring only two entities a voting entity and a server" the examiner respectfully disagrees.

As an initial matter the claims as recited do not identify what entity and/or entities are performing the method/system steps. For example Claim 29 merely recites "forming a digital signature of B_{cast} using a private key of the server $DS(B_{cast}, s)$".

Additionally, in Claim 29, the preamble states that the cast ballot is *stored* in a server it is not clear what, if any, of the method steps are performed/executed by the server or another entity. While one of the method steps recites "making the confirmation token available to a user" may imply that a user maybe involved in the method steps the user does not perform any action(s) on the confirmation token nor

does the claim positively recited an meaningful interaction/exchange with the user, thereby making the recitation that the confirmation token is made available to a user merely non-functional descriptive material.

Further it is noted that the features upon which applicant relies (i.e., an *architecture* limited to a *voting entity* and a server) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In contrast Shrader et al. clearly teaches a system and method for verifying a cast ballot comprising of a voting entity and a voting server/system wherein the voting system comprises at least two subsystems namely the voting tabulator and voting mediator (Figures 1a, depicts a single server/computer/system, 3).

In response to Applicant's argument that the prior art of record (Shrader et al.) fails to teach or suggest associating the cast ballot and server's digital signature of the cast ballot with a vote serial number the examiner respectfully disagrees.

Shrader et al. teach a system and method for verifying a cast ballot wherein each ballot (both prior to and after being cast) is assigned/includes a ballot identification number (ballot ID, vote serial number, etc.) for the purposes of unique identifying the vote/ballot and ensuring such things as no duplicated ballots are cast (Paragraph 0063; Certificate No., Figure 2).

In response to Applicant's argument that the prior art of record (Shrader et al.) fails to teach or suggest forming a confirmation token comprising the server's digital signature of the cast ballot and the vote serial number the examiner respectfully disagrees.

Shrader et al. teach forming a confirmation token comprising the server's/system's digital signature of the cast ballot and the vote serial number (by definition the cast ballot includes the ballot ID/VSN; Paragraph 0050-0053, 0063; Figure 8, Element 74) for the purposes of validating the message and ensuring that the ballot has not been cast more than once (which inherently requires the ability to uniquely identify the ballots).

In response to Applicant's argument that the prior art of record (Shrader et al.) fails to teach or suggest making the confirmation token available to a user, receiving the confirmation token made available to the user and subsequently extracting the vote serial number and the server's/system's digital from the received token and comparing the received server/system digital signature of the cast ballot to at least one of the server's/systems $DS(B_{cast},s)$ and $DS(B_{cast},S)$ the examiner respectfully disagrees.

Initially it is noted that the method step of making the confirmation token available to a user merely recites non-functional descriptive material as the method steps, data and/or the system are not altered and/or affected by the recited step, as discussed above, therefore the claims as written essentially state the generation, receipt and

subsequent verification of the token (message) as is clearly taught by Shrader et al. (Paragraphs 0061-0063; Figure 4, Elements 44-46; Figure 7, Elements 66-68; Figure 8).

In response to Applicant's argument that the prior art of record (Cranor et al. in view of Shrader et al.) fails to teach or suggest forming a digital signature of the cast ballot using the private key of the voter and forming a digital signature of the cast ballot using the private key of the server (i.e. different keys are used to form the two digital signatures) the examiner respectfully disagrees.

Initially it is noted that digitally signing a message (text, document, ballot, etc.) by definition is performed by the entity who is signing the message using their own private key wherein the entity's signature provides other entities the ability to do such things as verify that the digitally signed message was in fact signed by the entity (i.e. since only the entity signing a document knows their private key no other entity could sign the message); therefore it is implicit in the method and system for verifying a cast ballot as taught by the combination of Cranor et al. and Shrader et al. that each time an entity digitally signs a message (e.g. a ballot) they are using their private key (i.e. the digital signatures are created using different private key's).

Further Cranor et al. and Shrader et al. teach a system and method for verifying a cast ballot further comprising forming a digital signature of B_{cast} using the private key of the server (Cranor et al.: Paragraph 2, Page 5; Figures 1-3; Shrader et al.: Paragraphs 0050-0053, 0058-0060; "A digital signature uses the sender's private key to encrypt some portion of the message. When the message is received, the receiver

uses the sender's public key to decipher the digital signature as a way to verify the sender's identity and the integrity of the message.", Paragraph 0050; "each party participating in the voting transaction has a unique public and private key pair. As previously discussed, each key pair serves to protect and secure the transaction by providing the means to encrypt, decrypt, authenticate and validate information and verify sources and destinations of information.", Paragraph 0058).

In response to Applicant's argument that the prior art of record (Cranor et al. in view of Shrader et al.) fails to teach or suggest associating the cast ballot, voter's digital signature of the cast ballot and server's digital signature of the cast ballot with a vote serial number the examiner respectfully disagrees.

The system and method for verifying a cast ballot as taught by the combination of Cranor et al. and Shrader et al. teach associating the cast ballot, voter's digital signature of the cast ballot and server's digital signature of the cast ballot with a vote serial number (Cranor et al.: identification tag, ballot tag; Paragraph 1, Page 11; Figures 1-2; Shrader et al.: Paragraph 0061, 0063; Certificate No., Figure 2).

In response to Applicant's argument that the prior art of record (Cranor et al. in view of Shrader et al.) fails to teach or suggest a confirmation token comprising the voter's digital signature of the cast ballot, the server's digital signature of the cast ballot, the cast ballot, the vote serial number and the digital signature of the above elements the examiner respectfully disagrees.

The system and method for verifying a cast ballot as taught by the combination of Cranor et al. and Shrader et al. teach a confirmation token comprising the voter's digital signature of the cast ballot, the server's digital signature of the cast ballot, the cast ballot, the vote serial number and the digital signature of the aggregation (Cranor et al.: Paragraph 1, Page 11; Paragraph 2, Page 12; Shrader et al.: Paragraph 0061, 0063; Certificate No., Figure 2; Figures 7-8).

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 29-30 and 33 are rejected under 35 U.S.C. 102(e) as being anticipated by Shrader et al., U.S. Patent Publication No. 2002/0077887.

Regarding Claims 29 and 33 Shrader et al. teach a method and system for verifying a (cast) ballot recorded (saved, stored, executed, etc.) in a system (server) comprising (Abstract; Paragraphs 0050-0053; 0060-0063; Figures 4-8):

- forming (generating, creating, signing, encrypting, etc.) a digital signature of a (cast) ballot using the private key of a system (server; "The voting tabulator signs, encrypts and sends the encrypted electronic ballot to the voting mediator 72 in a message that is encrypted with the voting mediator's public key and singed with the validator's private key; Paragraph 0063; Figures 7-8, Element 72);

- associating (storing, linking, relating, etc.) the (cast) ballot, the voter's digital signature of the ballot with a ballot number (vote serial number, unique number/unique identifier, etc.; validating ballot request; Paragraph 0061; Figures 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71);

- forming a message (confirmation, string, receipt, acknowledgement, token, etc.) comprising a system's digital signature of the ballot and the ballot number (verification message(s) exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8);

- making the message available (verification message exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8);

- receiving the message (verification message(s) exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8, Elements 72-74);

- extracting (decrypting, stripping, de-signing, deciphering, etc.) the ballot number and the system's digital signature from the message (verification message(s) exchanged between tabulator to mediator; Paragraph 0063; Figures 7-8, Elements 73-75);

- for vote serial number comparing the system's digital signature of the ballot received to the system's digital signature of the ballot (Paragraphs 0061-0063; Figures 7-8); and

- if the comparison shows equivalency (match, consistency, equality, etc.) determining that (cast) ballot (message, token, etc.) is verified (valid, authentic, genuine, unaltered, secure, etc.; Paragraphs 0061, 0063; Figures 7-8).

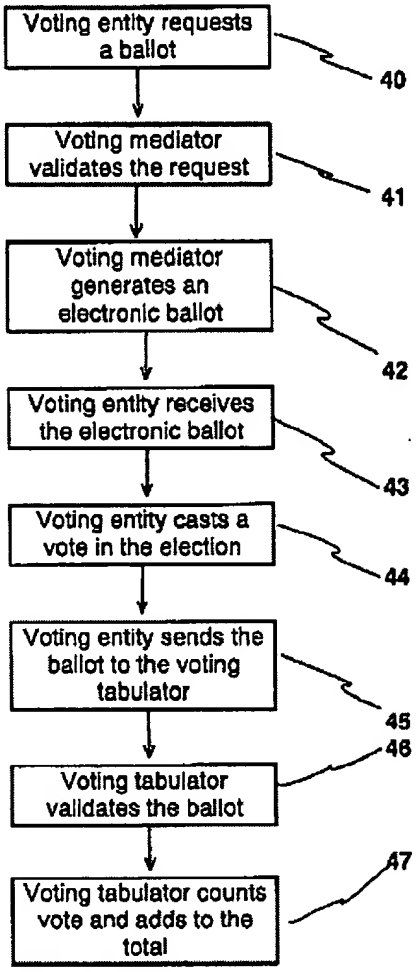
Voting entity requests a ballot
40
Voting mediator validates the request
41
Voting mediator generates an electronic ballot
42
Voting entity receives the electronic ballot
43
Voting entity casts a vote in the election
44
Voting entity sends the ballot to the voting tabulator
45
46
Voting tabulator validates the ballot
47
Voting tabulator counts vote and adds to the total

FIG. 4

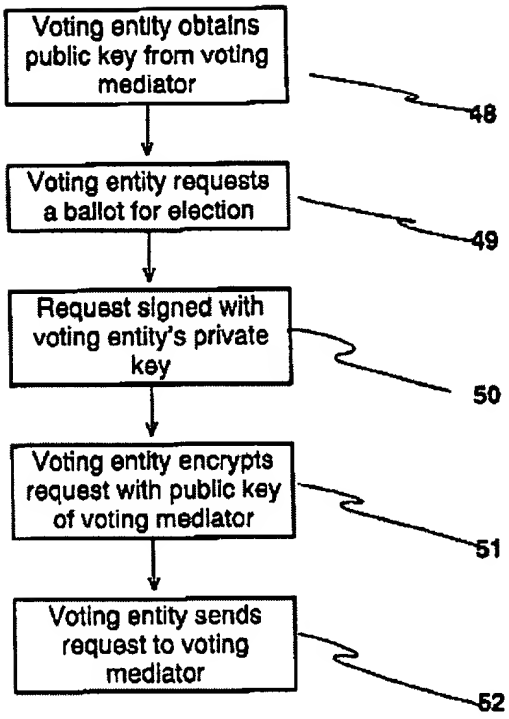
Voting entity obtains public key from voting mediator
48
Voting entity requests a ballot for election
49
Request signed with voting entity's private key
50
Voting entity encrypts request with public key of voting mediator
51
Voting entity sends request to voting mediator
52

FIG. 5

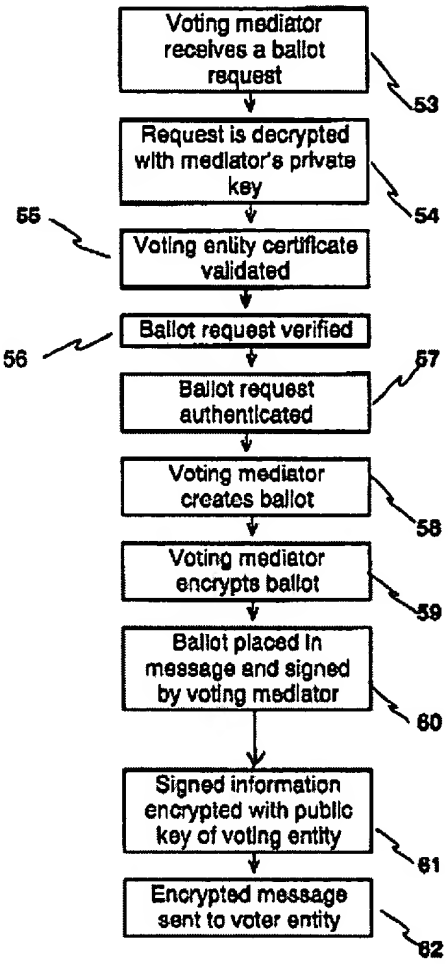
Voting mediator receives a ballot request
53
Request is decrypted with mediator's private key
54
55
Voting entity certificate validated
Ballot request verified
56
57
Ballot request authenticated
Voting mediator creates ballot
58
Voting mediator encrypts ballot
59
Ballot placed in message and signed by voting mediator
60
Signed information encrypted with public key of voting entity
61
Encrypted message sent to voter entity
62

FIG. 6

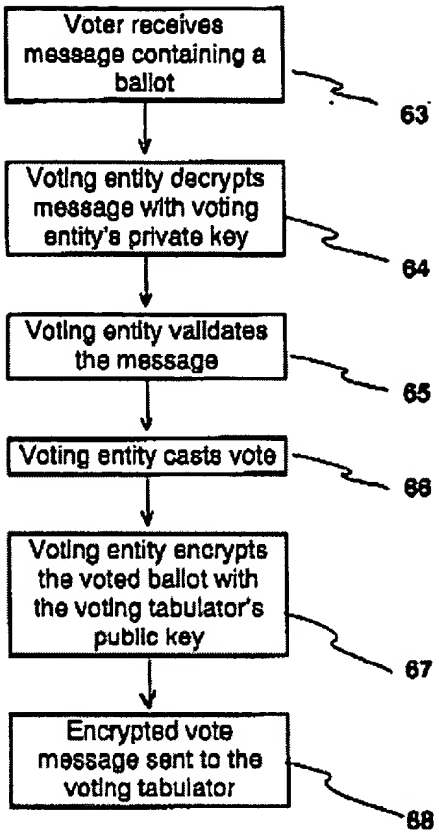
Voter receives message containing a ballot
63
Voting entity decrypts message with voting entity's private key
64
Voting entity validates the message
65
Voting entity casts vote
66
Voting entity encrypts the voted ballot with the voting tabulator's public key
67
Encrypted vote message sent to the voting tabulator
68

FIG. 7

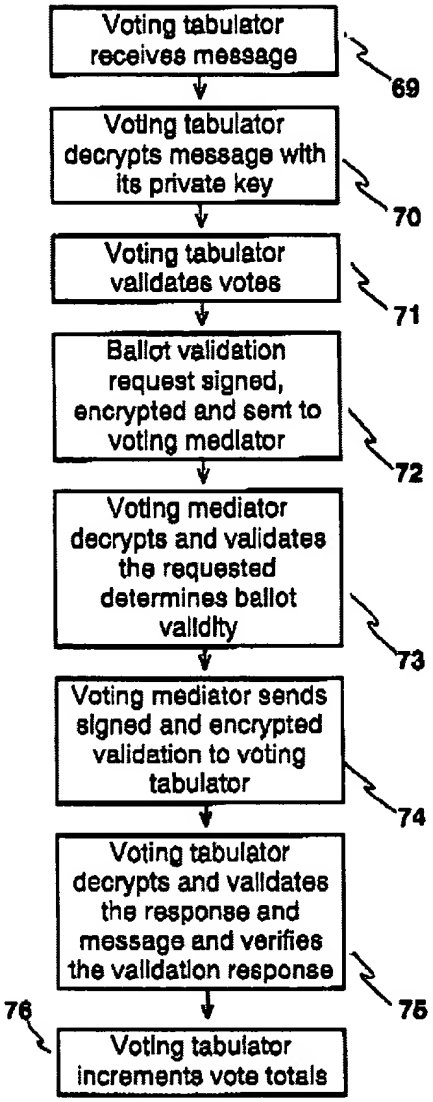

FIG. 8

Regarding Claim 30 Shrader et al. teach a method and system for verifying a ballot recorded in a system wherein the message (confirmation token, received token) further comprises the system's digital signature of the ballot and ballot number (aggregation; Paragraphs 0060-0062; Figure 2, Certificate No.); and wherein the method further comprises the steps of:

- extracting a digital signature of the ballot and ballot number (aggregation) from the message (received token; Paragraphs 0060, 0061, 0063; Figures 6-8); and

- the cast ballot is verified only upon the additional condition that the server's received digital signature of the aggregation is equivalent to the server's digital signature of the aggregation (Paragraphs 0061, 0063; Figures 6-8; Elements 67-75).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cranor et al., Design and Implementation of a Practical Security-Conscious Electronic Polling System (1996) in view of Shrader et al., U.S. Patent Publication No. 2002/0077887.

Regarding Claims 31 Cranor et al. teach a method and system for verifying (validating, authenticating, certifying, etc.) a cast ballot (vote) recorded (saved, stored, etc.) in a server (system) the method/system comprising (Abstract; Figures 1,3):

- receiving, in a system (server, computer, terminal, device, etc.), at least one set of a (cast) ballot and a voter's digital signature of the ballot (Paragraph 2, Page 5);

- forming (generating, creating, signing, encrypting, etc.) a digital signature of the ballot using the private key of a system (Paragraph 2, Page 5);

- associating (storing, linking, relating, etc.) the (cast) ballot, voter's digital signature of the ballot and the voter's identification number (Paragraphs 3-4, Page 7);

- forming a message (confirmation token, string, receipt, acknowledgement, etc.) comprising system's digital signature of the cast ballot, the voter's digital signature of

the cast ballot, and the system's digital signature of the aggregation of the cast ballot, the voter's digital signature of the ballot and the system's digital signature of the ballot ("validator", "tallier", "validation certificate", "receipt"; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1);

- making the message (token, string, etc.) available to a user (entity, voter, system, subsystem, third party, etc.; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1);

- receiving the messages (confirmation, token, verification, acknowledgement, etc.; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1);

- extracting (decrypting, stripping, etc.) *at least one of the following* from the message Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1):

  - voter's digital signature of the ballot;

  - system's digital signature of the ballot; ***or***

  - system's digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, ballot number (aggregation);

- for extracted ballot number and the corresponding ballot number comparing *at least one of the following* (Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1):

  - voter's digital signature of the ballot extracted from the message and voter's digital signature of the ballot;

- system's digital signature of the ballot extracted from the message and system's digital signature of the ballot, **or**
- system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, ballot number (aggregation) extracted from the message and system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, ballot number (aggregation); and

- if the comparison shows equivalency (match, consistency, equality, etc.) determining that the (cast) ballot is verified (valid, authentic, genuine, unaltered, accepted, counted, etc.; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1).

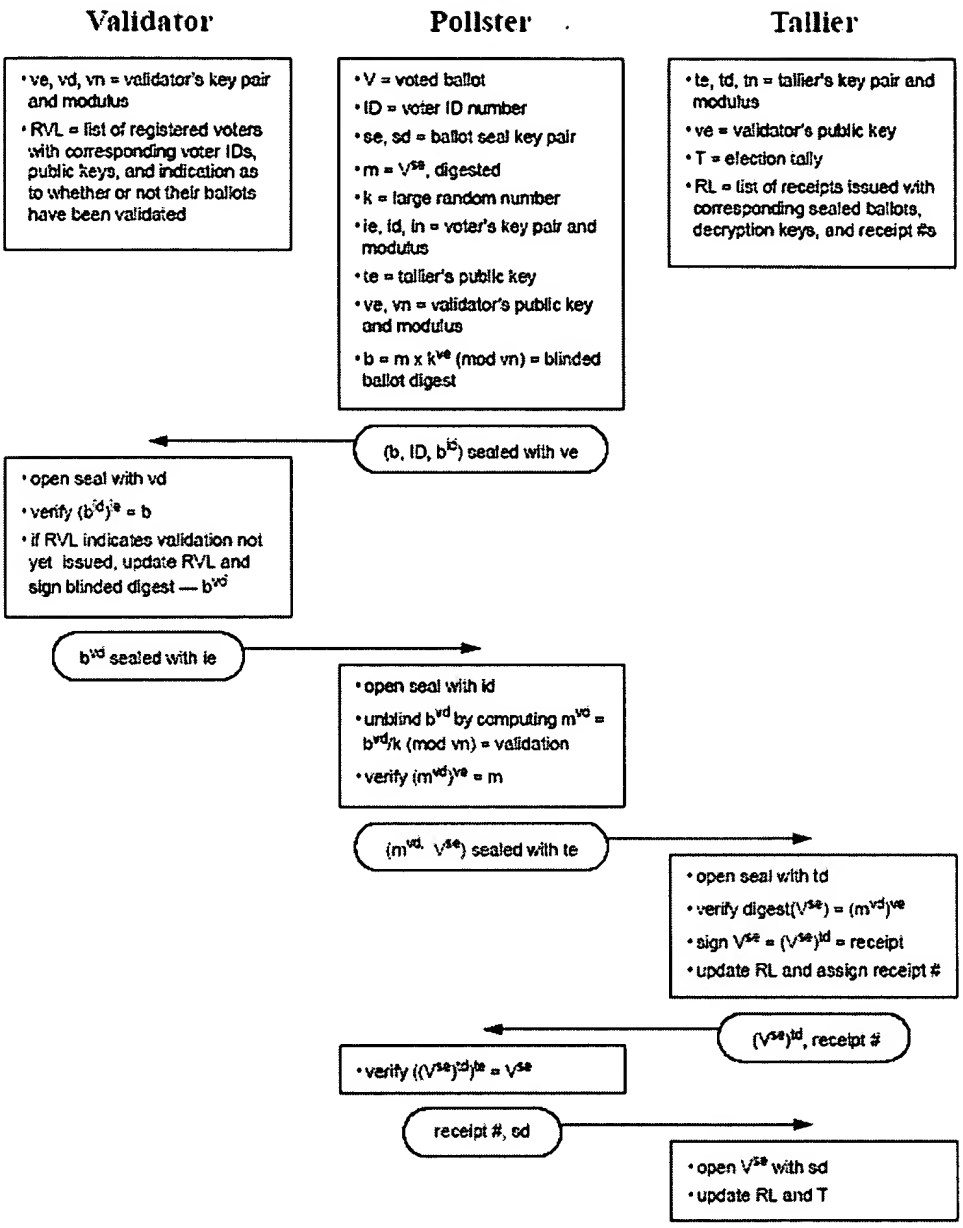

Figure 1: Blind Signature Protocol Overview

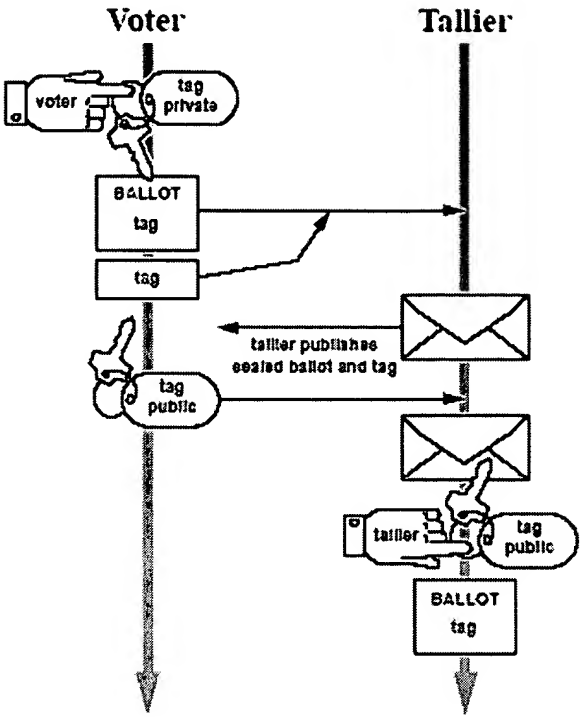

Figure 3: Phase 2 of the Two Agency Protocol

While the use of unique identifiers for (paper and/or electronic) ballots is a common practice Cranor et al. does not expressly teach that the cast ballot includes a vote serial number as claimed.

Shrader et al. teach that ballots comprise a vote serial number (unique ballot ID, certificate no.) in an analogous art of secure electronic voting/balloting over a network for the purposes of ensuring voters only cast their ballot once (Paragraph 0061; Figures 2, 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71).

It would have been obvious to one skilled in the art at the time of the invention that the system and method for verifying a cast ballot recorded on a system (server) as taught by Cranor et al. would have benefited from including in the ballot a unique ballot identifier (vote serial number) in view of the teachings of Shrader et al.; the resultant system/method providing an additional mechanism for ensuring that valid voters only vote once (Shrader et al.: Paragraph 0063).

Regarding Claim 32 Cranor et al. teach a method and system for verifying a cast ballot recorded in a system further comprising if the comparison shows equivalence between the system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, extracted from the message and system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot and the system's digital signature of the ballot (aggregation) determining that the message (token) has not been modified (altered, disturbed, edited, etc.) since its formation (Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8).

Cranor et al. does not expressly teach that ballots further comprise vote serial numbers as claimed.

Shrader et al. teach that ballots comprise a vote serial number (unique ballot ID) in an analogous art of secure electronic voting/balloting for the purposes of ensuring

voters only cast their ballot once (Paragraph 0061; Figures 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71).

It would have been obvious to one skilled in the art at the time of the invention that the system and method for verifying a cast ballot recorded on a system (server) as taught by Cranor et al. would have benefited from including in the ballot a unique ballot identifier (vote serial number) in view of the teachings of Shrader et al.; the resultant system/method providing an additional mechanism for ensuring that valid voters only cast their ballot once (Shrader et al.: Paragraph 0063).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Challener et al., U.S. Patent No. 6,081,793, teach a system and method for verifying a cast ballot having a ballot number which is encrypted and signed by the voter using well know public/private key encryption techniques/methods.

- Jakobsson, Bjorn Markus, U.S. Patent No. 6,317,833, teach a system and method for verifying a cast ballot wherein the cast ballot and an aggregation of the cast ballot and the digital signature are encrypted and signed by the voter and then subsequently verified/validated by the system.

- Fujioka et al., U.S. Patent No. 6,845,447, teach that in conventional electronic voting systems/methods voters encrypt and sign their cast ballots, which are then verified/validated by the system (election administrator). Fujioka et al. further teach a system and method for verifying/validating cast ballots, having serial numbers, using well-known cryptographic techniques such as public/private key encryption and digital signatures (e.g. signature verification includes the well known steps of comparing the results of a verification function).

- Neff, Andrew, U.S. Patent Publication No. 2002/0128978, teaches a system and method for verifying cast ballots, which are encrypted and signed by the voter using their private key and subsequently verified by the server/system for the purposes of detecting compromised/tampered with ballots. Neff further teaches making a confirmation token (receipt) available to a user/voting entity.

- Babbit et al., U.S. Patent Publication No. 2002/0019767, teach a system and method for conducting secure elections over the Internet comprising voter's encrypt and digitally sign cast ballots as well as voter's receiving a confirmation message/token comprising the cast ballot and the verification/authentication of the cast ballot by the server/system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Scott L. Jarrett whose telephone number is (571) 272-7033. The examiner can normally be reached on Monday-Friday, 8:00AM - 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hafiz Tariq can be reached on (571) 272-6729. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SJ
9/10/2006

Romain Jeanty
Primary Examiner
Art Unit 3623